FORTINET
High Performance Network Security

FortiADC™ Deployment Guide

Load Balancing FortiMail

FORTINET DOCUMENT LIBRARY

http://docs.fortinet.com

FORTINET VIDEO GUIDE

http://video.fortinet.com

FORTINET BLOG

https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT

https://support.fortinet.com

FORTIGATE COOKBOOK

http://cookbook.fortinet.com

FORTINET TRAINING SERVICES

http://www.fortinet.com/training

FORTIGUARD CENTER

http://www.fortiguard.com

END USER LICENSE AGREEMENT

http://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK

Email: techdocs@fortinet.com

November 03, 2015

FortiADC Deployment Guide: Load Balancing FortiMail

Revision 2

TABLE OF CONTENTS

Change Log

Date	Change Description
2015-09-08	Initial release.
2015-11-03	Updated configuration of FortiMail interface.

Introduction

For years, cybercriminals have used email to personalize attacks, tricking victims as a means to increase success. The proliferation of Advanced Persistent Threats (APTs) and other forms of stealth malware have taken targeted attacks to a whole new level, and it's only going to get worse. Cybercriminals are becoming more sophisticated as they strive for greater return on their investments. Phishing emails are becoming more personalized. They target victims by organization, language, region, city, or interest group.

Cybercriminals have long relied on email as a vehicle to deliver infected PDFs, .exe files, and other malicious attachments. That's not going to change. What will likely change, however, is the technical sophistication of the attached malware. While numerous reports have noted that overall spam levels have decreased, the number of emails that come with malicious code attached is on the rise.

FortiMail has always been at the forefront of email threat mitigation. Fortinet is the first vendor to combine cutting-edge anti-spam techniques with anti-virus detection, real-time behavioral analysis, and malware URL detection.

And now, combined with the FortiADC solution, Fortinet delivers a complete highly redundant solution that eliminates the need for complicated policy based routing (PBR) on external routers. This high performance email security solution protects your network against inbound attacks, including advanced malware, while improving application performance and server availability. The combination not only enables customers to stay one step ahead of threats, it also enhances quality of experience (QoE) for your end users.

Solution benefits

- Highly redundant solution that avoids complicated policy based routing configuration on routers
- Delivers 99.999% application uptime with intelligent server load balancing
- Advanced traffic steering (TCP, UDP, and more)
- Increase overall performance
- Improve user QoE (quality of experience)
- Full security coverage (FortiGuard, Integrated DLP, Antispam, Anti-malware, and much more…)
- Unparalleled deployment flexibility

The FortiADC difference

There are a number of hardware load balancing products available on the market with a wide range of features and capabilities. FortiADC differentiates itself by providing superior value, high performance, reliability, advanced acceleration features, and security from a market leader.

FortiADC not only load balances Internet service requests across multiple servers, but also accelerates application performance and provides application-aware features that monitor server load and improve server response times – by as much as 25%. In addition to basic load balancing, FortiADC provides:

- Automatic server and application health monitoring.
- Intelligent, application-aware load balancing policies (least connections, fastest response time, static weight, and round robin).
- Redundant high availability (HA) configurations.
- Intuitive Layer 7 policy-based routing that can dynamically rewrite content to support complex applications and server configurations.
- Hardware and software-based SSL offloading that reduces the performance impact on your server infrastructure.
- Content caching that dynamically stores popular application content, such as images, videos, HTML files, and other types to alleviate server resources and accelerate overall application performance.
- Web Application Firewall protects against application layer attacks.
- IP Reputation service that protects your applications against automated web attacks by identifying access from botnets and other malicious sources.
- Global Server Load Balancing that distributes traffic across multiple geographical locations for disaster recovery.
- Link Load Balancing that distributes traffic over multiple ISPs to increase resilience and reduce the need for costly bandwidth upgrades.
- Authentication offloading that speeds user authentication for secure applications.
- Scripting for custom load balancing and content rewriting rules.
- Virtual domains (VDOMs) that enable administrators to divide a FortiADC into two or more virtual FortiADC devices, each operating as an independent application delivery controller.

For more information on how FortiADC can make your applications work better, faster, and more economically, please visit http://www.fortinet.com/products/fortiadc/index.html.

The FortiMail difference

FortiMail appliances and virtual appliances are proven, powerful email security platforms for any size organization—from small businesses to carriers, service providers, and large enterprises. Purpose-built for the most demanding messaging systems, FortiMail appliances employ Fortinet's years of experience in protecting networks against spam, malware, and other message-borne threats. FortiMail can be deployed to address important security concerns, such as:

- Detect sensitive information using defined data patterns and ensure secure delivery with no additional hardware or software to install, no user provisioning, no recipient pre-enrollment.
- Apply data loss prevention (DLP) and identity-based encryption.
- Prevent phishing and other advanced threats.
- Identify and block spamming endpoints.
- Anti-virus and malware detection.
- Integration with FortiSandbox and FortiGuard analytics for advanced threat protection – Emails are queued by FortiMail while FortiSandbox inspects the email contents for threats.
- Content-based protection.
- Dictionary-based filtering in inbound or outbound direction.
- Filter by attachment file type.
- Denial-of-service protection.
- Inbound and outbound message rate limiting.
- Identity-based encryption for push/pull delivery of encrypted messages.
- Support for strong-crypto protocols, including HTTPS, SMTPS, SSH, IMAPS, and POP3S.

For more information on how FortiMail can address your email security concerns, please visit http://www.fortinet.com/products/fortimail/index.html.

Solution deployment topology

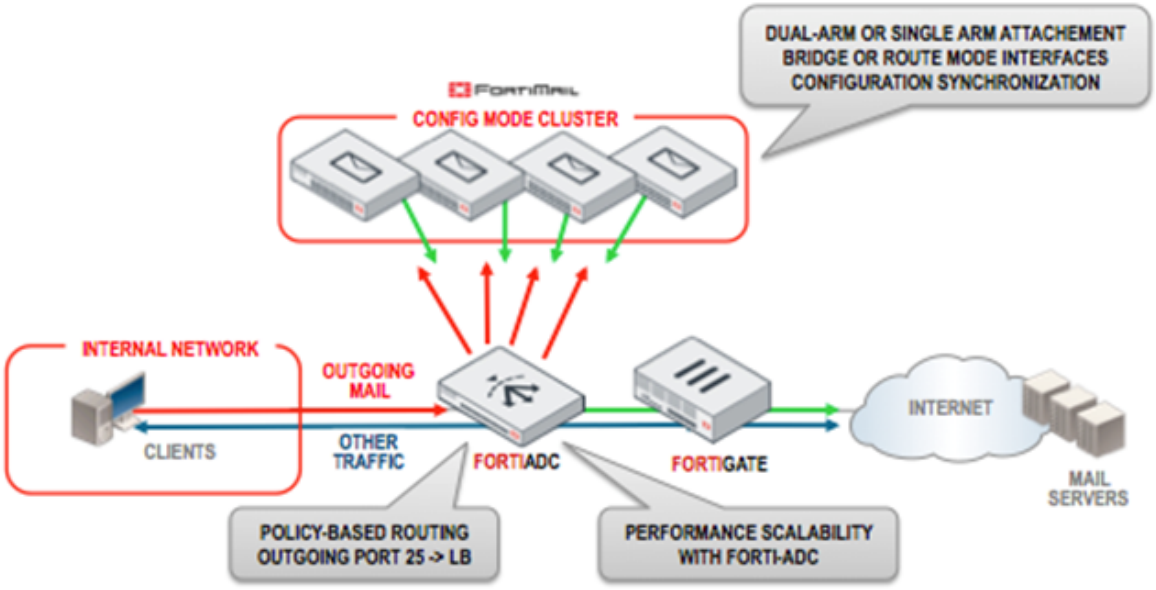
FortiADC can be deployed to load balance traffic to FortiMail appliances in two ways:

- Layer 3 One-Arm mode—Traffic is load-balanced through a cluster of FortiMail units configured in Transparent Proxy (Layer 3) mode with one interface (one-armed). Each FortiMail units act as a Layer 3 router, intercepting and scanning SMTP traffic.
- Layer 3 Two-Arm mode—Traffic is load-balanced through a cluster of FortiMail units configured in Transparent Proxy (Layer 3) mode with two different interfaces (two-armed). Each FortiMail units act as a Layer 3 router, intercepting and scanning SMTP traffic.

In this guide, we describe a Layer 3 One-Arm mode deployment.

Logically, FortiADC is deployed between clients accessing the SMTP server and the Exchange servers, as shown in the following diagram. FortiADC redirects SMTP traffic to the FortiMail according to a FortiADC link load balancing (LLB) policy.

Figure 1: Solution deployment topology



SMTP traffic coming from the Internal network through real servers must follow this sequence:

Forward Path

- Client-X to FortiADC
- FortiADC to FortiMail-X (a member of FortiMail cluster)
- FortiMail-X to FortiADC
- FortiADC to Server-X

Reverse Path

- Server-X to FortiADC
- FortiADC to FortiMail-X (same unit as in forward path)

- FortiMail-X to FortiADC
- FortiADC to Client-X

Hardware and software used in this example

The following hardware and software were used in testing this example:

- FortiADC VM
- FortiADC OS Version 4.3
- FortiMail 60D
- FortiMail OS Version 5.2
- Custom client/server hardware running VMware ESX 4

Important: This guide is written only for the FortiADC D-series platform. The instructions included within are not designed to be used with the FortiADC E-series platform application delivery controllers.

FortiADC configuration

This section provides FortiADC configuration guidelines. The granular configuration framework requires that you configure policy objects in a particular order. This configuration includes the following steps:

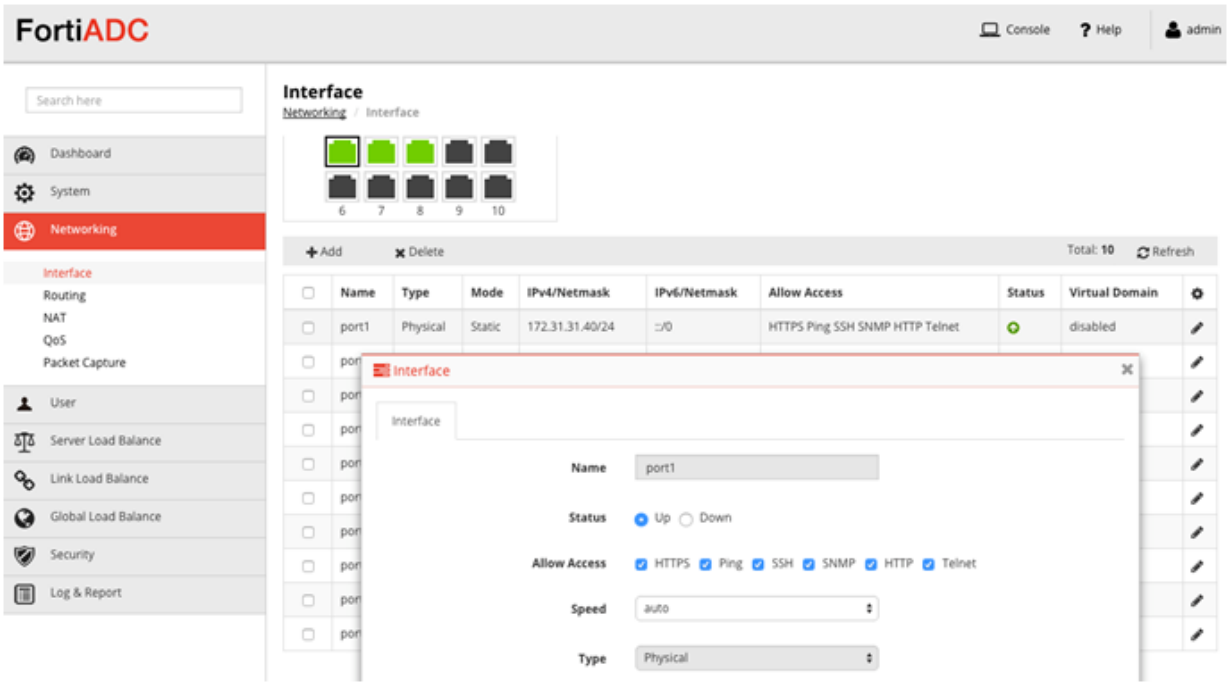
Step 1: Configure network interfaces and a static route

For a one-arm deployment, you configure three interfaces:

- port1—Internal network (LAN)
- port2—Redirect SMTP traffic to FortiMail
- port3—External network (WAN)

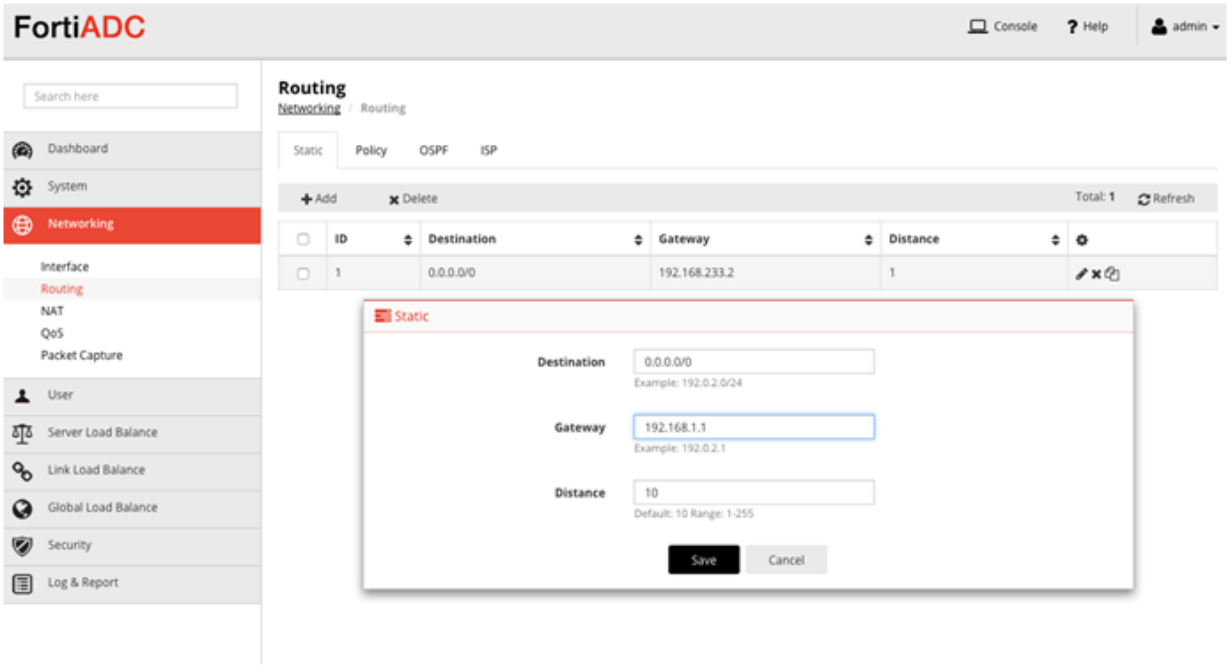
To configure network interfaces, go to Networking > Interface. Figure 2 shows the configuration for port1.

Figure 2: Network interface configuration page



To create a static route, go to Networking > Routing. Figure 3 shows the static route configuration page.

Figure 3: Static route

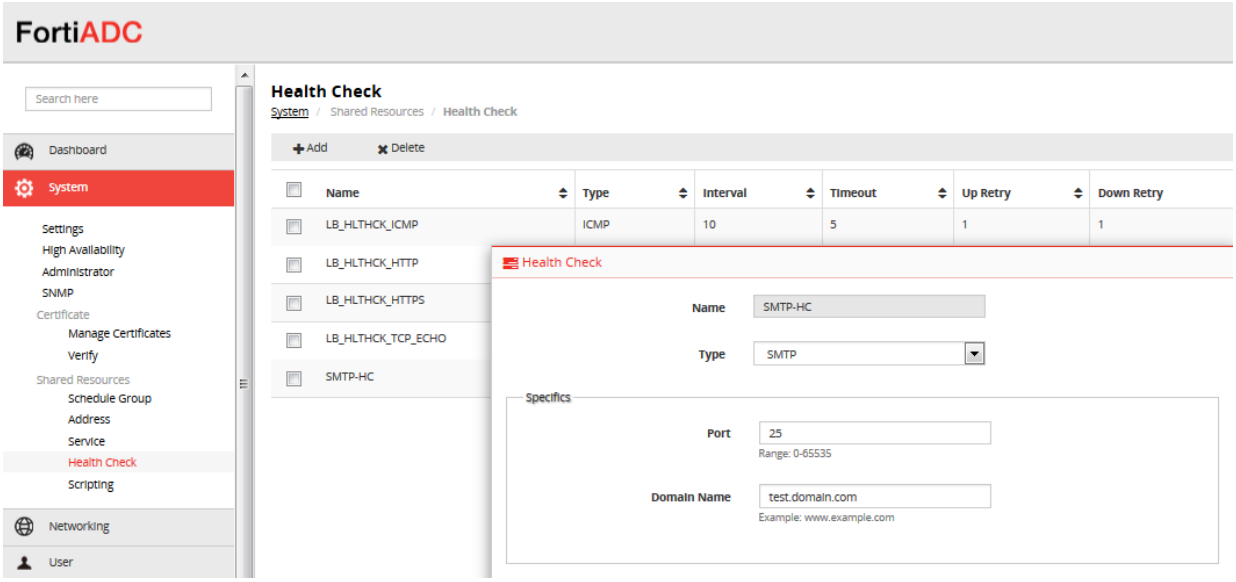


Step 2: Configure health checks

Health checks test gateway or server availability. When you configure an SMTP health check, you specify a FQDN, such as test.domain.com, to use in the SMTP HELO request that is periodically sent to test server response. If the response is OK (250), the server is considered as up. If there is error response (501) or no response at all, the server is considered down.

To configure a health check, go to System > Shared Resources > Health Check. Figure 4 shows the SMTP health check configuration for this example.

Figure 4: Health check configuration page

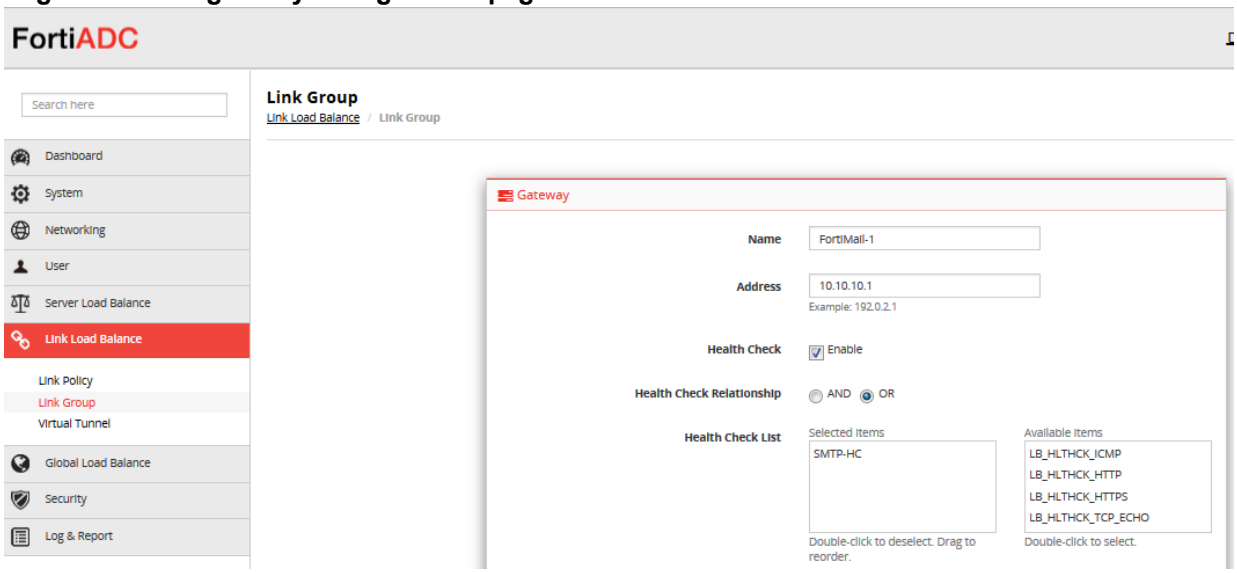


Step 3: Configure LLB gateways

In this deployment, the FortiADC link load balancing (LLB) feature is used to load balance traffic to FortiMail appliances. In the LLB framework, gateways are the pool of links that are loadbalanced. Create a gateway object for each FortiMail appliance, specify its IP address, and select the health check configured in the previous step.

To configure LLB gateways, go to Link Load Balance > Link Group > Gateway. Figure 5 shows an LLB gateway configuration used in this example.

Figure 5: LLB gateway configuration page

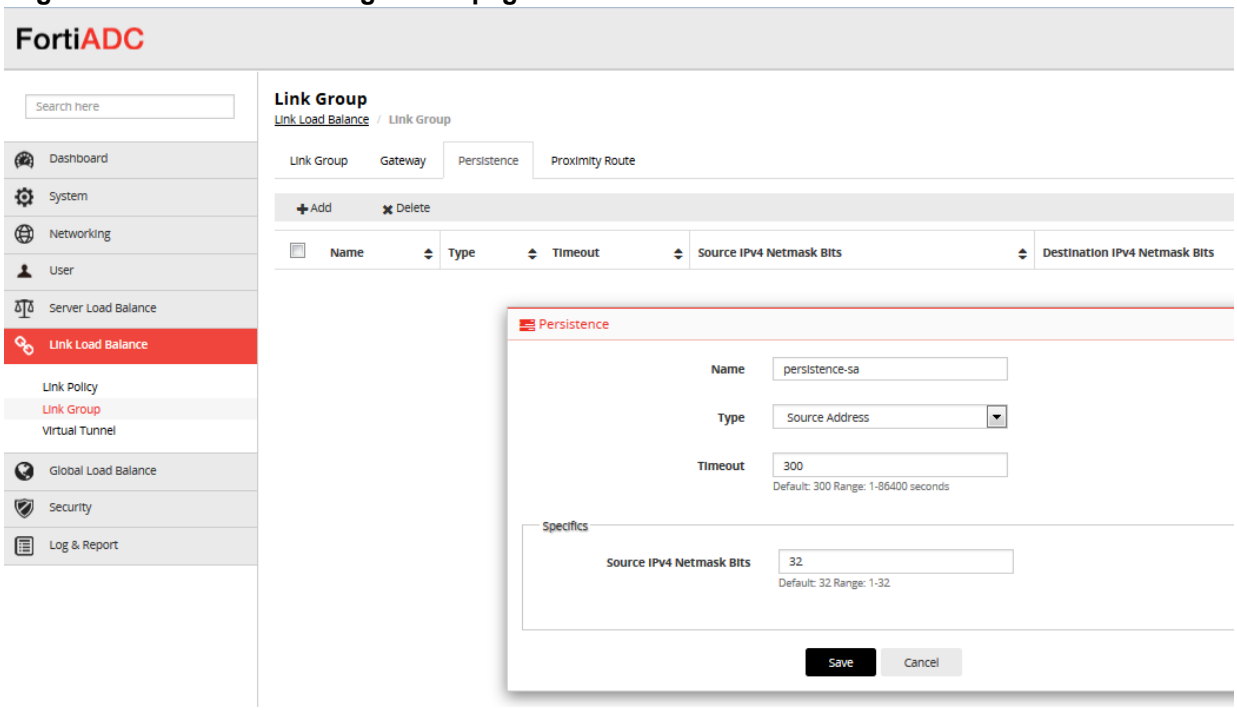


Step 4: Configure persistence rules

Persistence rules identify traffic that should be ignored by load balancing rules and instead be forwarded to the same gateway each time the traffic traverses the FortiADC appliance. You should use persistence rules with applications that use a secure connection. Such applications drop connections when the server detects a change in a client's source IP address. This deployment uses Source Address persistence. Packets with a source IP address that belongs to the same subnet take the same outgoing gateway.

To configure persistence rules, go to Link Load Balance > Link Group > Persistence. Figure 6 shows the configuration used in this example.

Figure 6: Persistence configuration page



Step 5: Configure link groups

Link groups are the pools of LLB gateways that are load balanced. The link group general settings configuration specifies the load balancing method and persistence method. The link group member configuration specifies the weight.

To configure an LLB link group, go to Link Load Balance > Link Group. When you configure general settings, select the persistence object created in the previous step. When you add members, select the FortiMail "gateways" configured in the previous step.

Figure 7 shows the link group configuration page. Figure 8 shows the member configuration page.

Figure 7: Link group configuration page

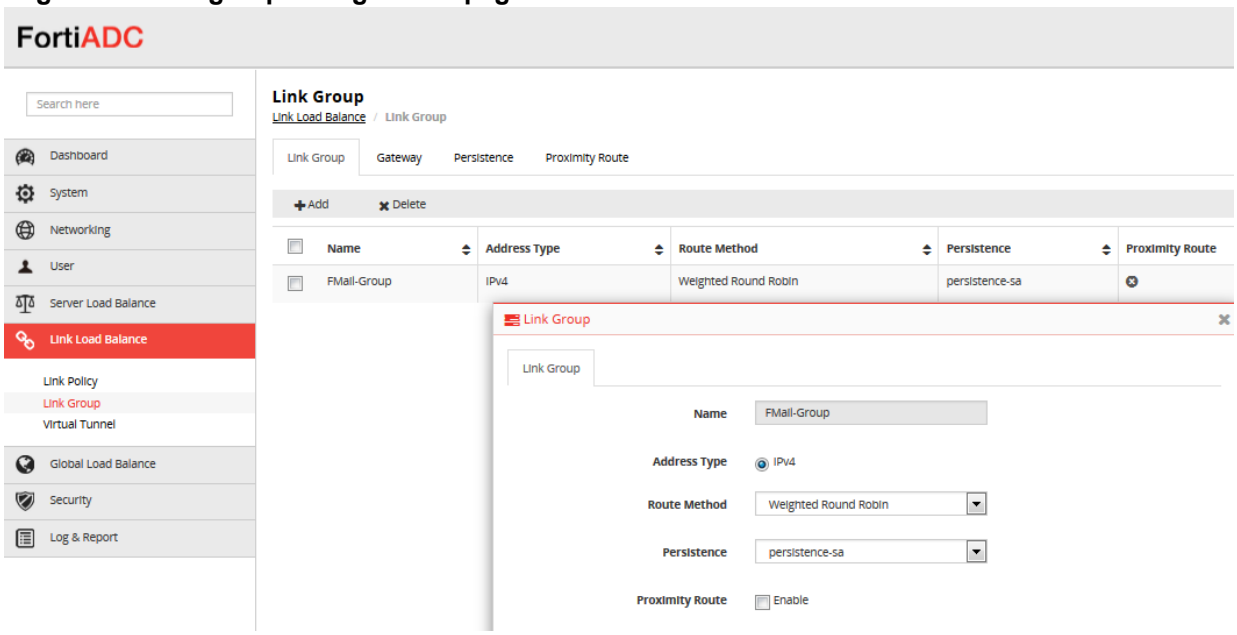
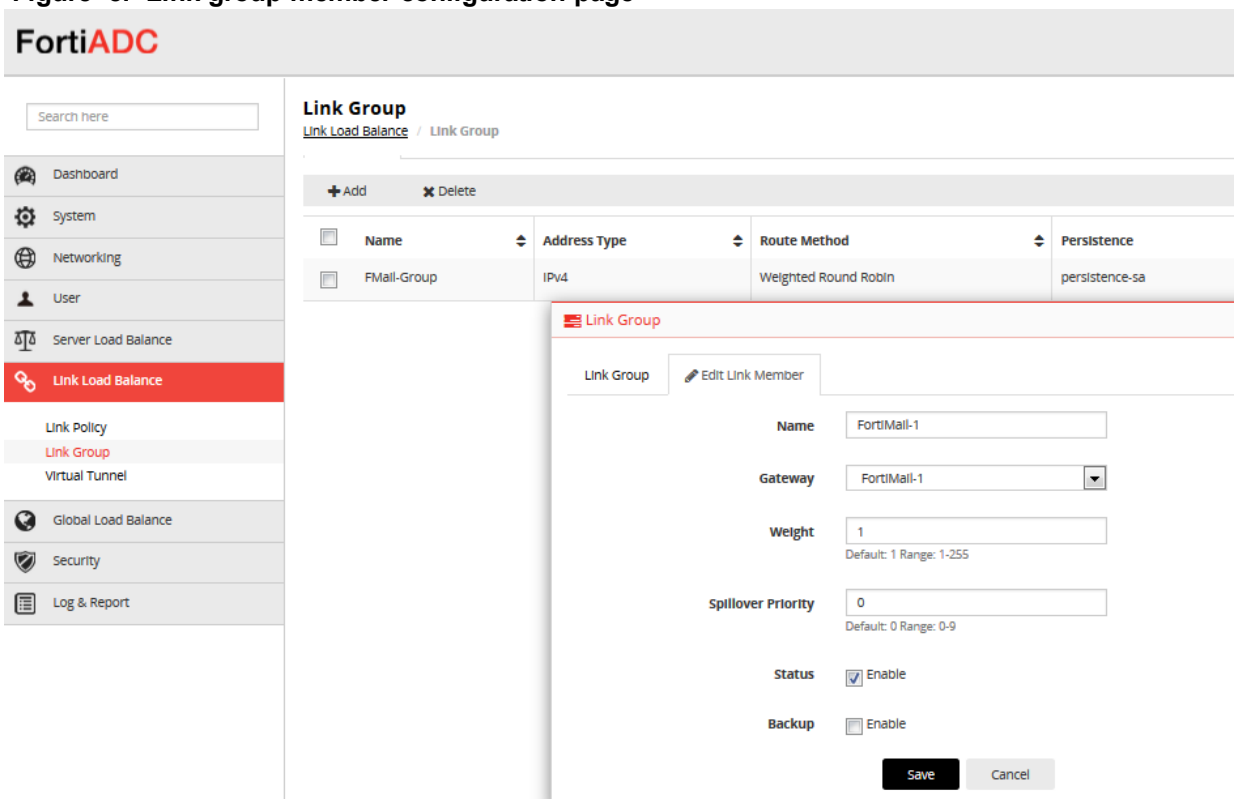


Figure 8: Link group member configuration page



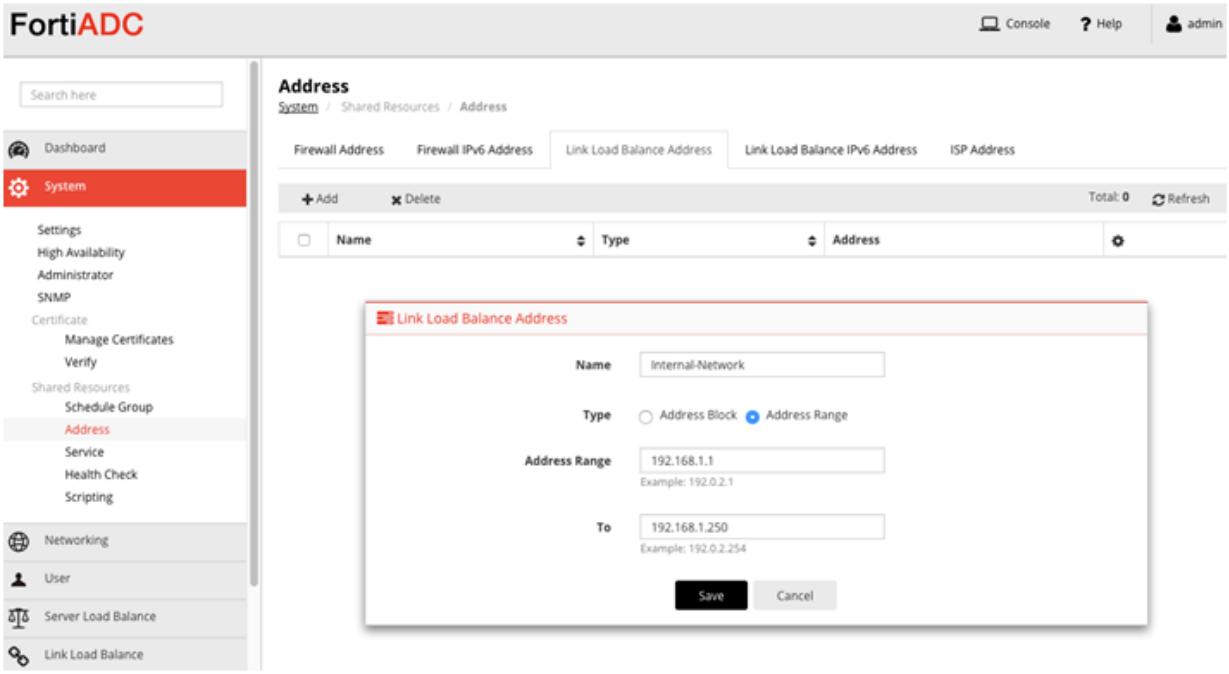
Step 6: Configure LLB policy address objects

An LLB policy is a traffic steering policy that matches traffic to link groups. The match criteria include source address, destination address, service, and schedule. All must match for the rule to be applied.

To configure the address objects for the policy, go to System > Shared Resources > Address. Figure 9 shows an address configuration for this example.

Note: You do not have to create an address object for the wildcard ANY. To match any source or destination address in the policy, simply leave the setting empty.

Figure 9: LLB policy address object configuration page



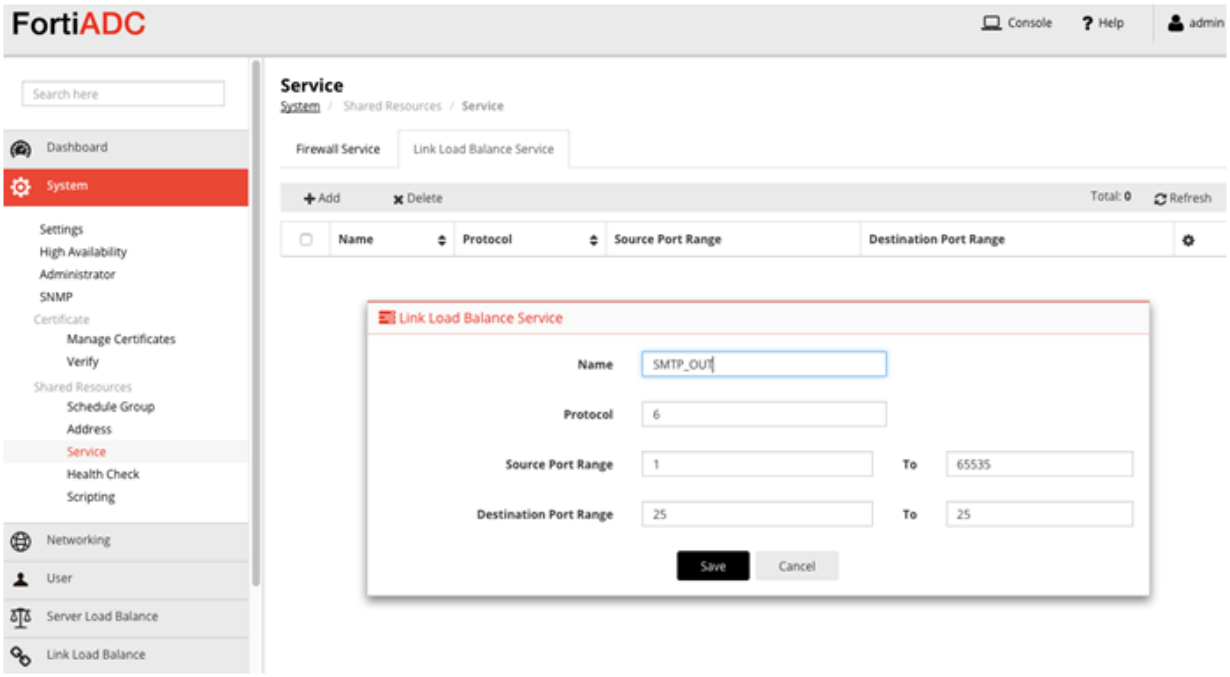
Step 7: Configure LLB policy service objects

An LLB policy is a traffic steering policy that matches traffic to link groups. The match criteria include source address, destination address, service, and schedule. All must match for the rule to be applied.

To configure the service objects for the policy, go to System > Shared Resources > Service. Figure 10 shows a service configuration for SMTP. The configuration sets protocol 6 (TCP) and destination port 25 (SMTP). In this example, create an object for SMTP outbound (destination port 25) and one for return traffic (source port 25).

Note: You do not have to create an address object for the wildcard ANY. To match any service in the policy, simply leave the setting empty.

Figure 10: LLB policy service object configuration page



Step 8: Configure LLB policies

An LLB policy is a traffic steering policy that matches traffic to link groups. The match criteria include source address, destination address, service, and schedule. All must match for the rule to be applied.

This example uses two rules:

- Egress —Matches traffic initiated from the internal network to the outside (www). Matching traffic is redirected to a FortiMail link group member.
- Ingress—Matches traffic returning from the outside (www) to the internal network. Matching traffic is redirected to a FortiMail link group member. The persistence setting ensures traffic is redirected to the same FortiMail address as the initial ingress session.

To configure LLB policies, go to Link Load Balance > Link Policy.

Figure 11 shows the egress rule. The source address match is the address object for the internal network. The destination match is any (empty). The service match is the object for destination port 25 (SMTP). Matching traffic is redirected to the FortiMail link group. The particular FortiMail address is determined by the results of health checks, the load balancing method or persistence rule, and group member weight.

Figure 11: LLB policy egress rule

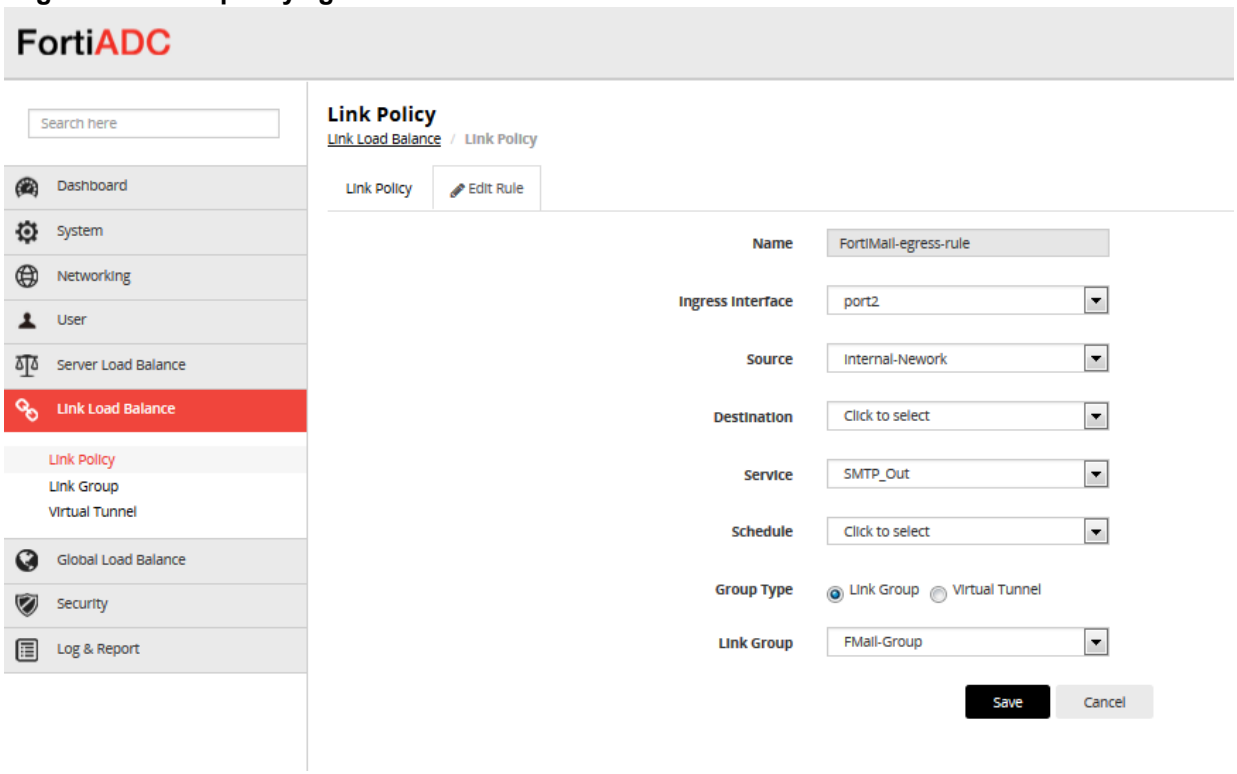
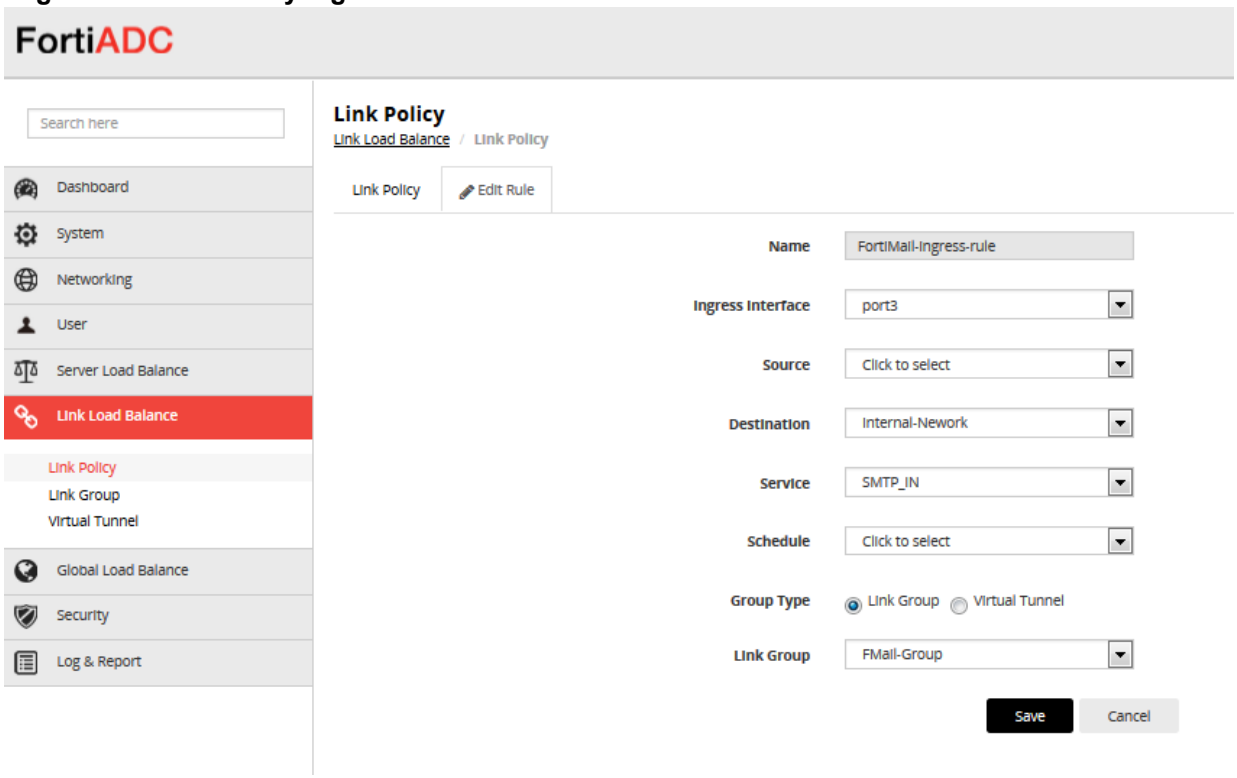


Figure 12 shows the rule for return traffic. The source address match is any (empty). The destination match is the internal network address object. The service match is the object for source port 25 (SMTP). Matching traffic is redirected to the FortiMail link group. The particular FortiMail address is determined by the results of health checks, the load balancing method or persistence rule, and group member weight.

Figure 12: LLB Policy ingress rule



FortiMail configuration

This section provides FortiMail configuration guidelines. The configuration includes the following steps:

Step 1: Configure operation mode

In a one-arm deployment like this example, you deploy FortiMail in Transparent mode.

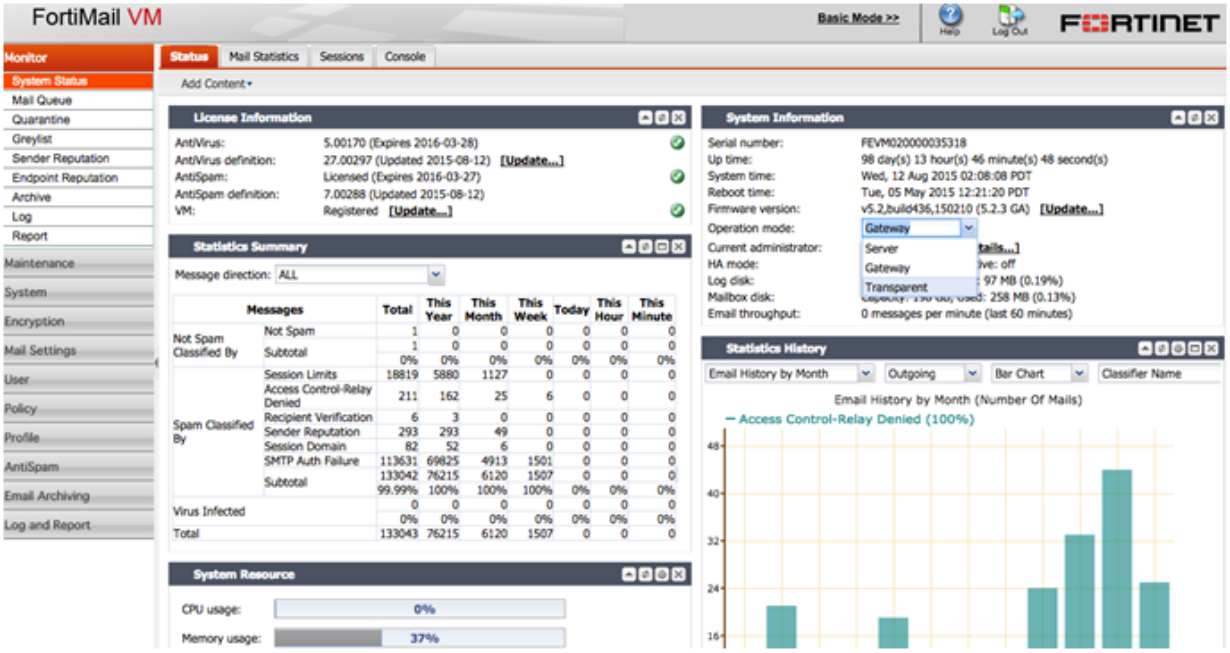
Note: In Transparent mode, all ports are members of the transparent bridge. Be careful not to create a loop in your network. We recommend you disable unused ports to avoid looping.

To configure operation mode:

1. Go to Monitor > System Status.
2. In the System Information portlet, set operation mode to **Transparent**.
3. Click **Yes** to reboot FortiMail.

Figure 13 shows the operation mode setting.

Figure 13: FortiMail operation mode configuration



Step 2: Configure network interfaces and a static route

In a one-arm deployment, you configure just one interface to receive traffic from FortiADC and return traffic to FortiADC. You specify a static route with the FortiADC IP address as the next hop for return traffic.

To configure the interface, go to System > Network > Interface. Figure 14 shows the configuration page. Note the following key settings:

- Do not associate with management IP—Select this option to enable FortiMail to intercept email traffic.
- SMTP Proxy—Select **Proxy** outgoing connections. This enables FortiMail to intercept only outgoing email.

Figure 14: FortiMail interface configuration

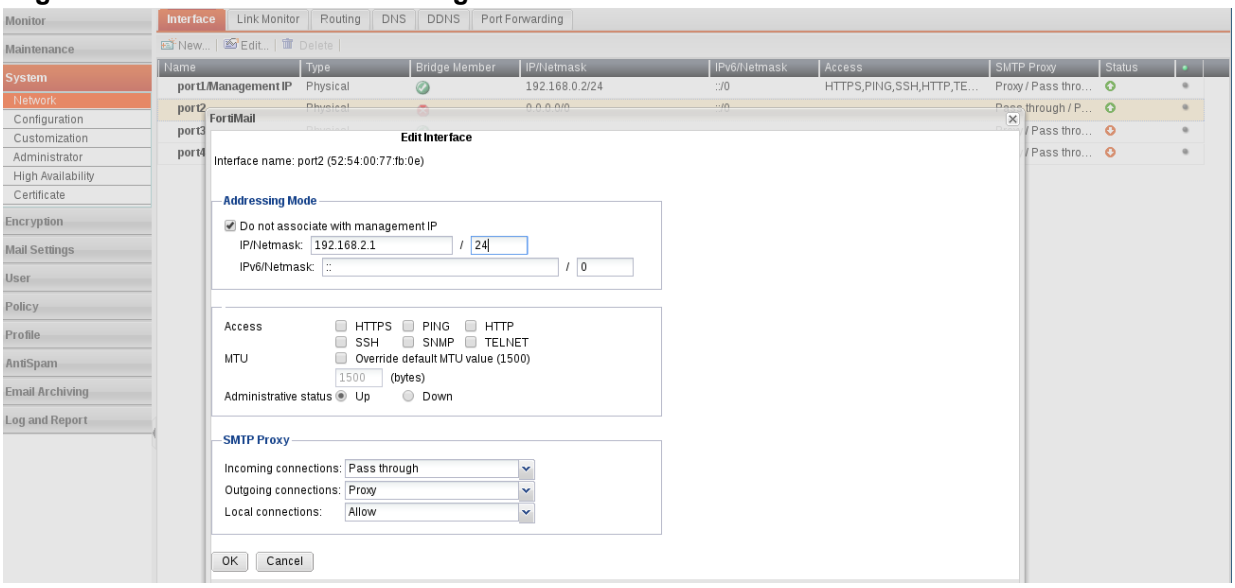
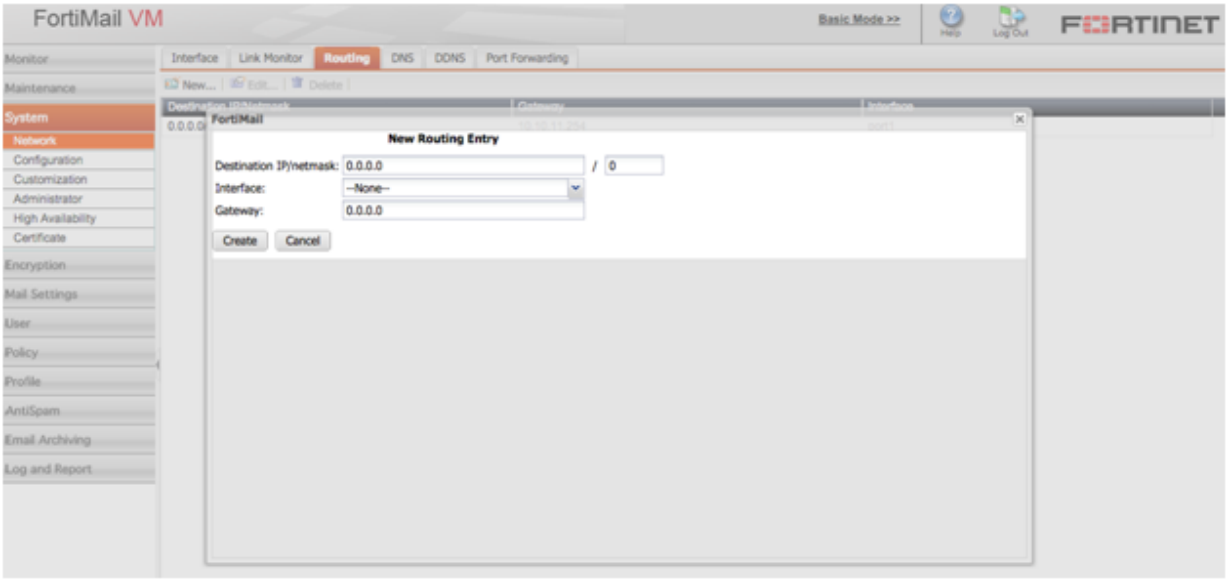


Figure 15 shows the static route configuration page. Specify the FortiADC address as the next hop gateway.

Figure 15: FortiMail static route configuration page

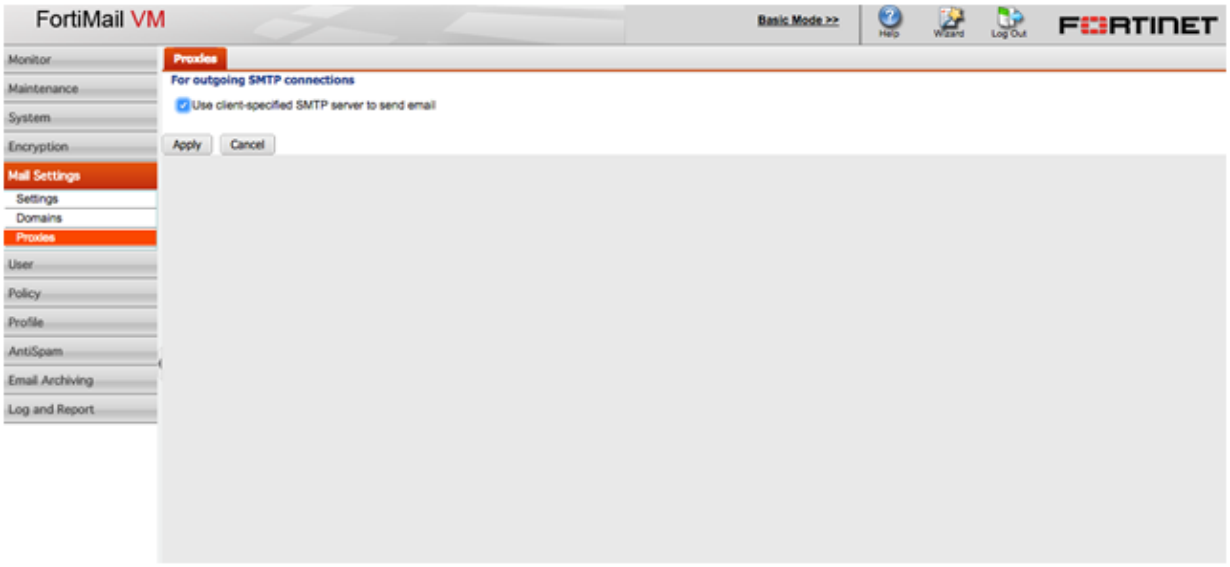


Step 3: Enable Transparent Proxy

FortiMail can transparently proxy or relay email traffic to and from the email servers that it protects. This eliminates the need to change the existing email server network configuration.

To enable transparent proxy, go to Mail Settings > Proxies. Figure 16 shows the configuration for this example. The **Use client-specified SMTP server to send email** option is enabled.

Figure 16: FortiMail transparent proxy configuration



Step 4: Enable Source IP Spoofing

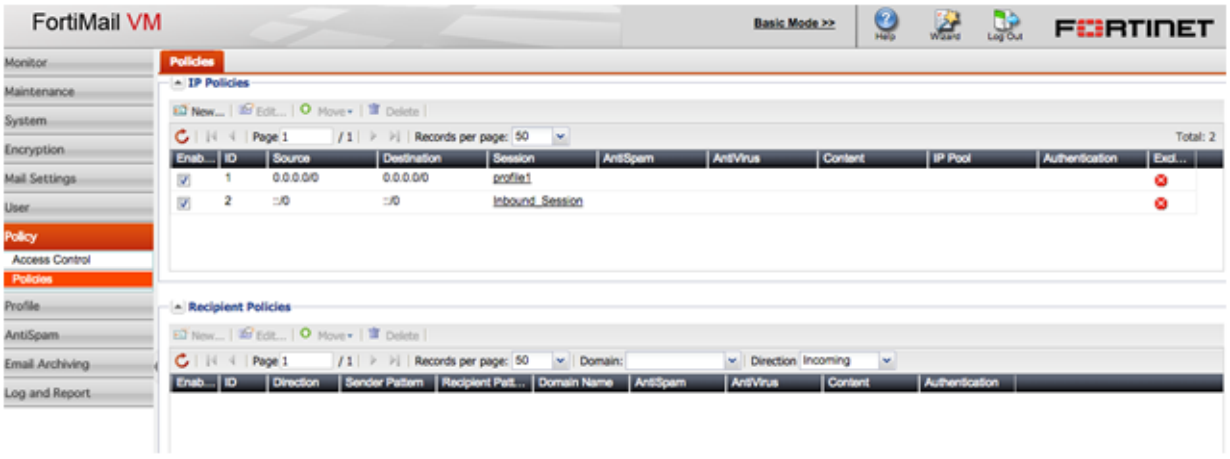
The FortiMail built-in message transfer agent (MTA) and proxies are not necessarily fully transparent, even if FortiMail is deployed in Transparent mode. By default, the source IP address of connection initiations, the destination IP address of reply traffic, and the SMTP greeting (HELO/EHLO) will contain one of the following:

- The management IP address (for connections occurring through bridged network interfaces)
- The network interface IP address (for connections through out-of-bridge network interfaces)

You must select the **Hide this box from the mail server** profile option to hide these details.

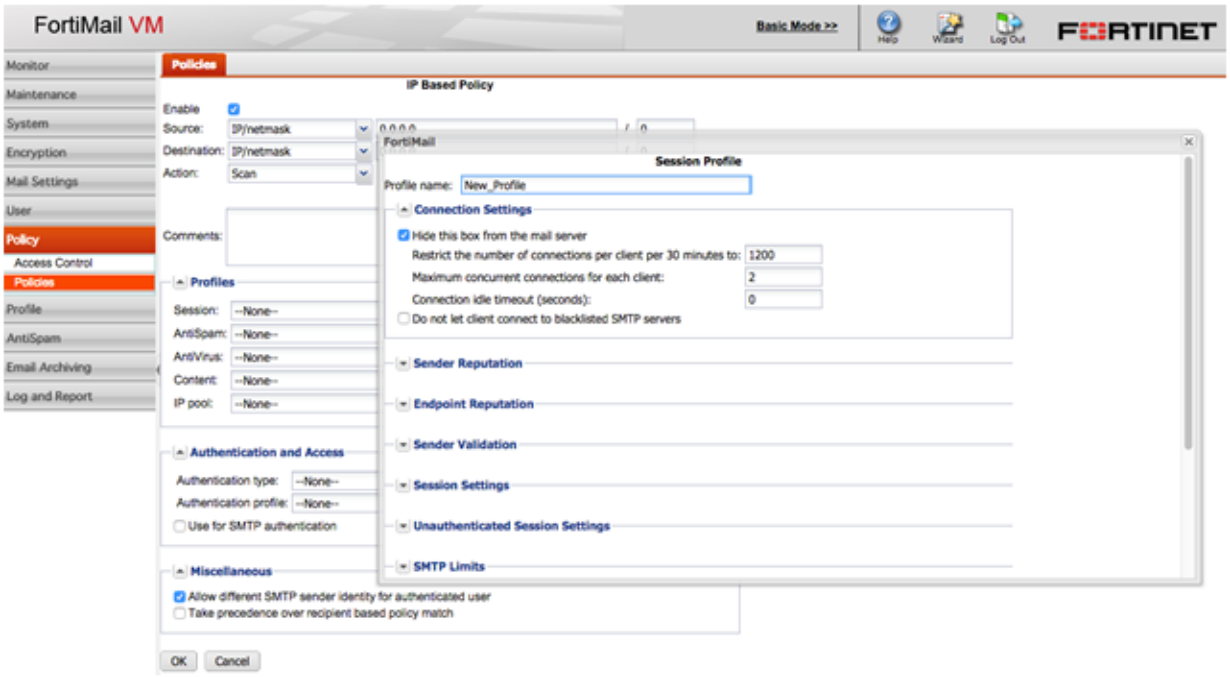
To configure this setting:

1. Go to Policy > Policies to display the policy list.



2. Edit the first row (ID 1, 0.0.0.0/0).

3. In the Profile table, go to Session and click **New** to display the profile editor.



4. Select the **Hide this box from the mail server** profile option.
5. Save the configuration.